HOW TO: Proof of Concept

One-Arm (Sniffer) Mode

Fortinet LATAM SE Team

Version 1.6

December 2013

DOCUMENT CHANGES LOG

Version	Author	Date	Change(s)
1.0	Marcelo Mayorga	Sep 5, 2013	Main document template, FortiGate configuration
1.1	Marcelo Mayorga	Sep 9, 2013	Changed Template, FortiAnalyzer configuration
1.2	Marcelo Mayorga	Sep 22, 2013	Report Generation
	Vadin Corrales		Fixed errors and added comments
1.3	Marcelo Mayorga	Nov 7, 2013	Added reference
	Vadin Corrales		Fixed errors and added comments
1.4	Marcelo Mayorga	Dec 11, 2013	Updated document to FortiAnalyzer 5.0.5
	José Luis Laguna Merino		Added check-list section
	Matteo Arrigoni		Content fixes
1.5	Marcelo Mayorga	Dec 13, 2013	Changed on report generation section, Added customer report import “Application and Risk Analysis – One Arm”
	Martin Hoz		Added disclaimer and some content correction
1.6	Marcelo Mayorga	Dec 18, 2013	Fixed minor changes
	Martin Hoz		Fixed errors, added content on disclaimer, benefits and drawbacks and others

CONTACT

For comments or suggestions about this document, please contact document coordinator Marcelo Mayorga (mmayorga@fortinet.com)

DISCLAIMER

This documents is intended for Fortinet engineers with experience on information security, networking and at least one year configuring FortiGate and FortiAnalyzer, using version 5 of their respective operating systems.

This document is NOT intended for end users or people not used to install and/or operate network security technology.

Fortinet, its employees and affiliates are not responsible for any service affection or impact that could be generated while doing any activity described in this document.

INTRODUCTION

DOCUMENT GOAL

The goal of this document is to provide a guideline on how to do a Proof of Concept (POC) and show how a network might be protected, without the necessity of building a complete working vehicle for that purpose. This is achieved by means of FortiGate capability of acting as a one-arm device in the network.

PREPARE YOURSELF

Similar to what happens in an actual product deployment, the success of a Proof of Concept is extremely tied to a proper and responsible planning. Before doing any action, make sure you:

1) Call the customer, gather and set expectations
2) Gather and document information, credentials, IP address schemes, etc.
3) Products are registered and have a valid contract (See: “Registering your unit” below).
4) Make sure paperwork and administrative tasks have been done. Remember some companies require approval in order to allow gear to get into their premises or insert it into their network.
5) Last but not least, make sure you know the entire process. Try the whole procedure at least once on a controlled environment (may be your own company network). The last thing you want to do is to look doubtful in front of a potential customer!

SNIFFER MODE / ONE-ARM / SPAN MODE – BENEFITS AND DRAWBACKS

Before getting into the technical stuff is important to understand that deploying a FortiGate in a one-arm topology has benefits and drawbacks.

NOTE

On this document the terms *sniffer*, *one-arm* and *span* modes are used interchangeably

Benefits:

- Non-intrusive: Does not require mayor changes nor will affect network performance.
- Provides real-time visibility of customer's traffic
- Allows a customer (prospect) to familiarize with Fortinet's GUI without the associated risk of interfering with production traffic.

Drawbacks:

- Not valid for sizing or performance measurement: Processing traffic in sniffer mode does not demand the same kind and amount of resources as it takes doing inline inspection.
- It does not provide (and shouldn't be positioned as) security protection. The focus is on visibility
- Some traffic might not be caught and some FortiGate inspection features won't work on this mode.
- SSL Inspection is not supported in sniffer mode.

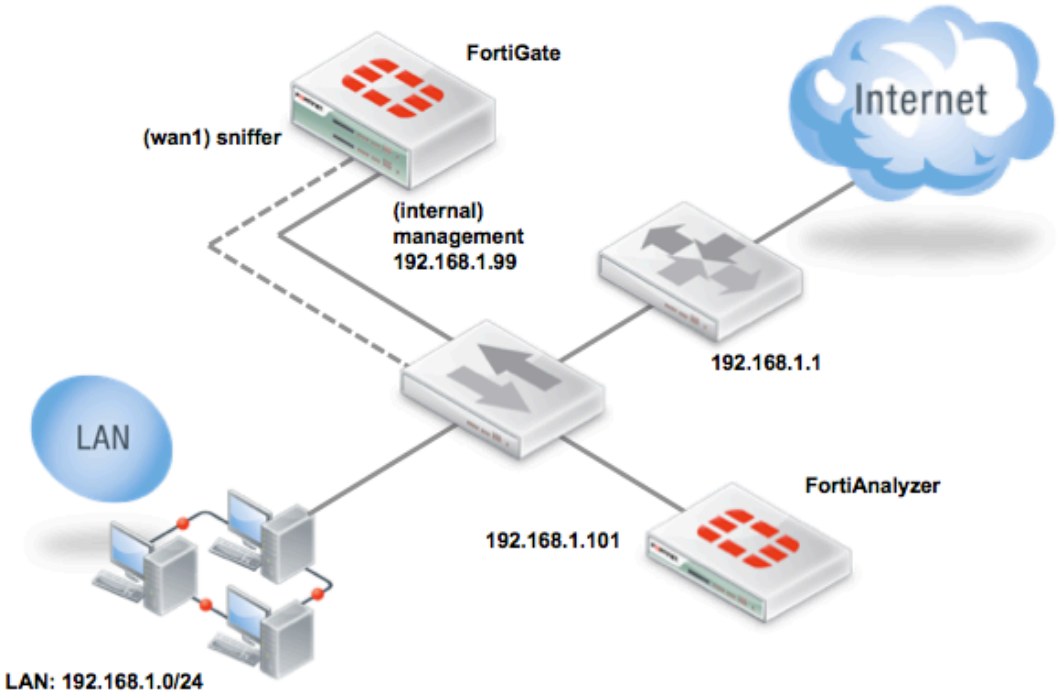
REQUIRED GEAR AND VERSIONS USED

For this document, the following versions were used.

- FortiGate: This document was created using FortiOS 5.0.4 (build0228).
- FortiAnalyzer: This document was created using FortiOS 5.0.5 (build0266).

While the hardware models used on this document are a FortiGate 60C and a FortiAnalyzer VM, It is recommended to properly size the right hardware. If in doubt, size like if the FortiGate were going to do full inline inspection and the FortiAnalyzer were to receive full logging.

NETWORK TOPOLOGY



REGISTERING YOUR UNIT

Remember that your FortiGate unit must be registered within Fortinet Support system in order to be able to access FortiGuard services and thus updating its security databases (AV, IPS, Applications, etc.).

For a detailed guide on how to register a Fortinet product, read the following document: https://support.fortinet.com/Download/RegistrationGuide.pdf

TYPOGRAPHIC CONVENTIONS

Whenever you see this:

```
CLI
```

It means the following steps can be done using the Command Line Interface

Whenever you see this:

```
GUI
```

It means the following steps can be done using the Graphical User Interface

HANDS-ON: FORTIGATE CONFIGURATION

This document has been created starting from a factory default configuration. If you're not an experienced user we recommend you to restore your FortiGate to defaults before moving on. Of course, a previous backup might be wise.

1. Connect to your FortiGate either through CLI (SSH/Telnet/Console) or using the embedded CLI Console widget in FortiGate's GUI
2. Execute:

CLI

```
# exec factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)y
```

CONFIGURING MANAGEMENT INTERFACES

With default configuration, login to the FortiGate and configure one interface to be used for management purpose.

NOTE

Default management interface will depend on FortiGate model. If you don't know which interface to use, take a look to corresponding QuickStart Guide: http://docs.fortinet.com/

Default management IP address: 192.168.1.99

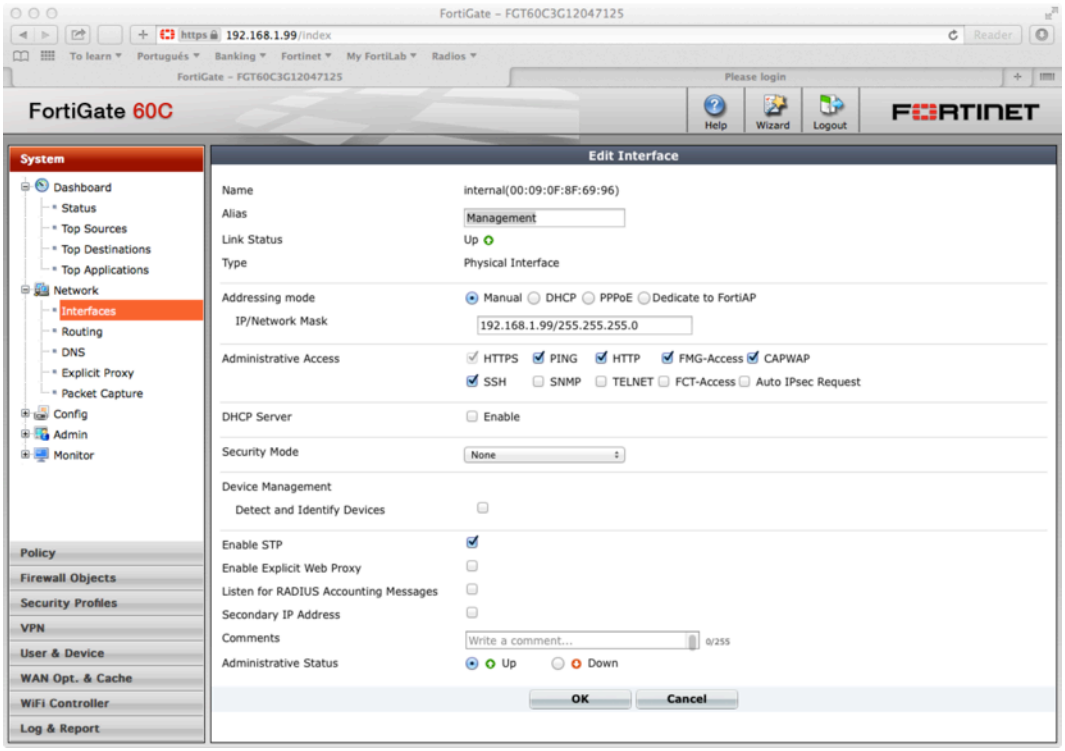
Login credentials: admin/<blank password>

CLI

```
config system interface
    edit "internal"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
        set allowaccess ping https ssh http fgfm capwap
        set type physical
        set alias "Management"
        set snmp-index 1
    next
end
```

GUI

1. Go to System → Network → Interfaces
2. Select appropriate management interface.
3. Configure IP/Mask
4. OK



Remember that your FortiGate must reach FortiGuard servers in order to do Web Filtering, update IPS/AV databases and engines.

Configure DNS Servers and routing in order to reach the Internet.

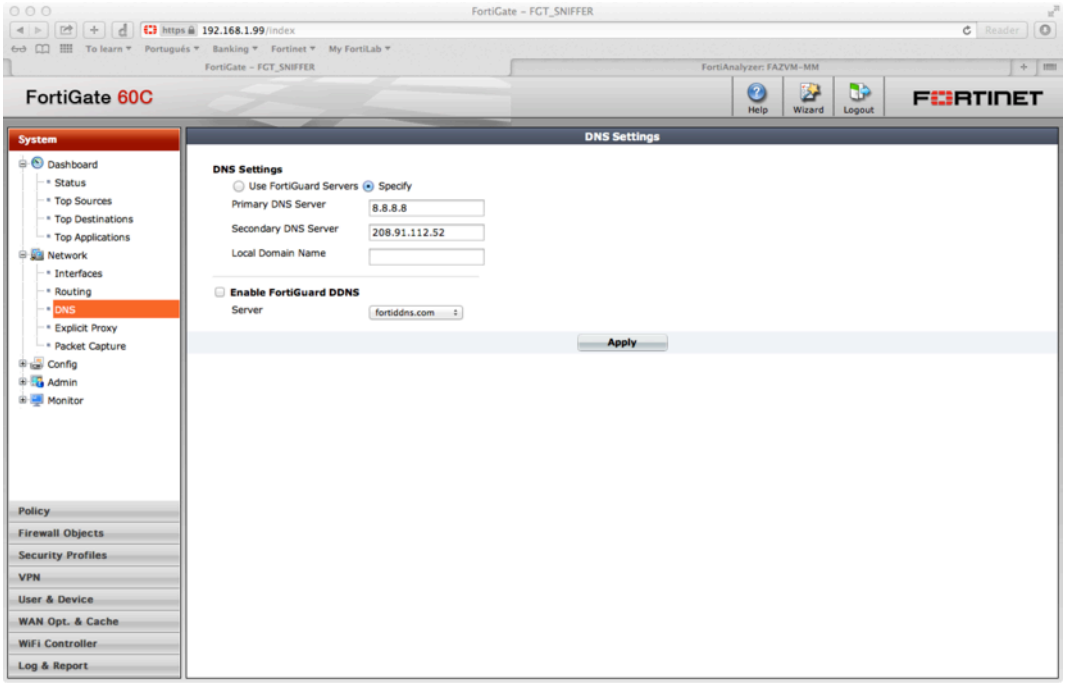
CONFIGURE DNS SERVERS:

CLI

```
config system dns
    set primary 8.8.8.8
    set secondary 208.91.112.52
end
```

GUI

1. Go to System → Network → DNS
2. Configure Primary and Secondary DNS
3. Apply



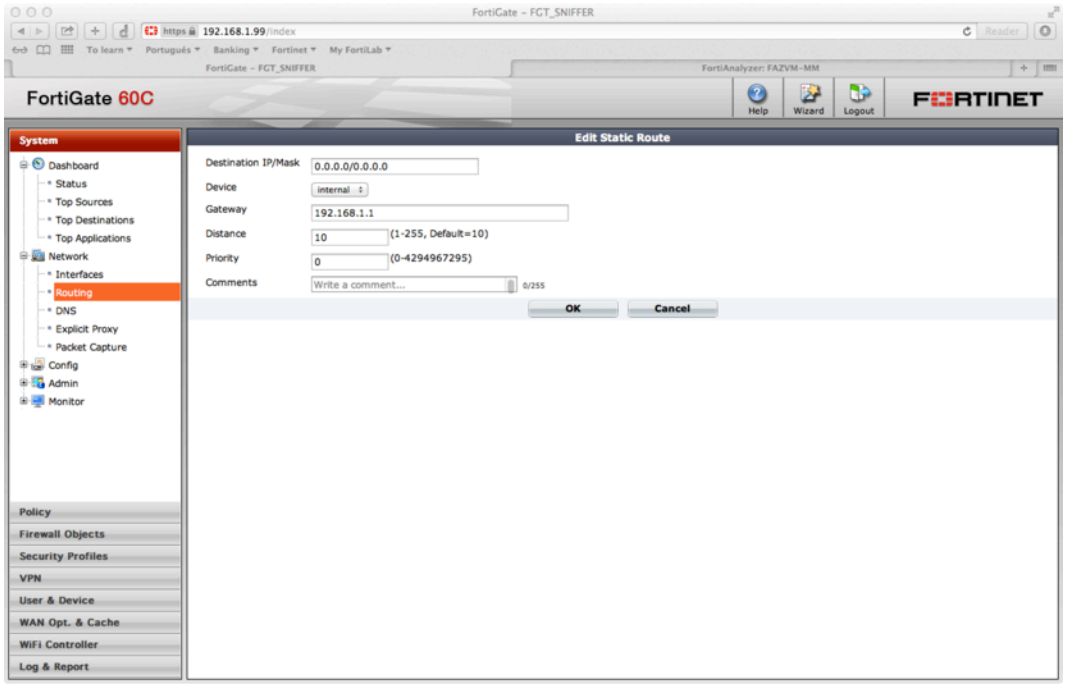
CONFIGURE DEFAULT GATEWAY

CLI

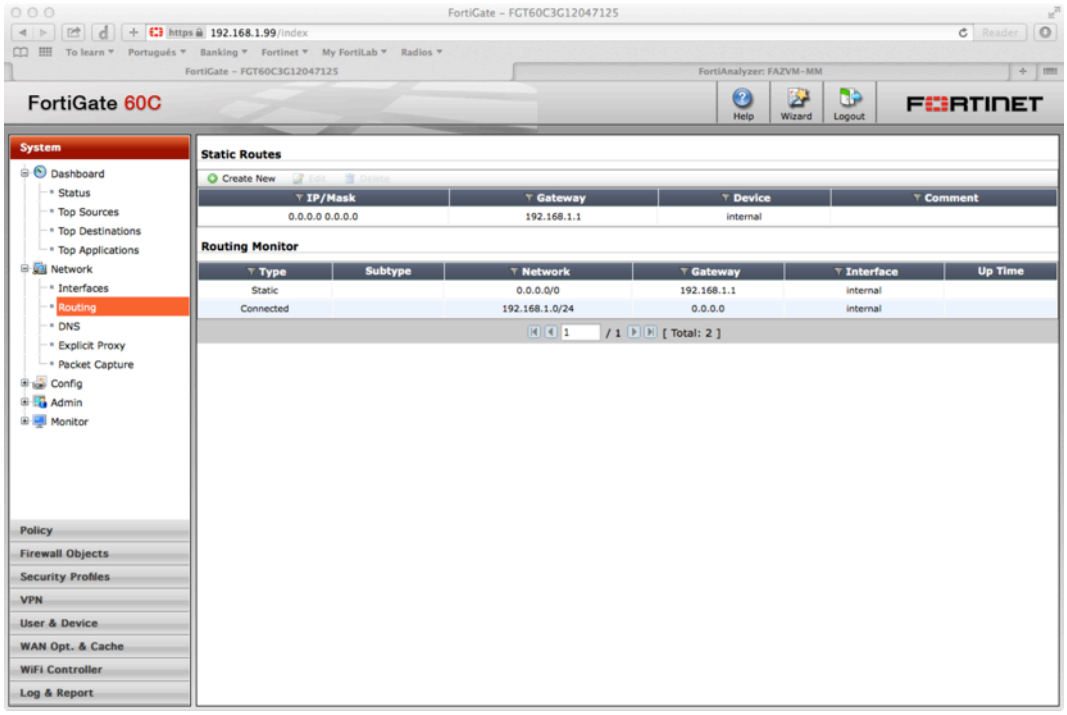
```
config router static
    edit 0
        set device "internal"
        set gateway 192.168.1.1
    next
end
```

GUI

1. Go to System → Network → Routing
2. Under Static Routes: Create New



3. Add Gateway and outgoing Device (i.e. interface facing default gateway).
4. OK



VERIFY ROUTING TABLE

CLI

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 192.168.1.1, internal
C       192.168.1.0/24 is directly connected, internal
```

Verify you are able to reach an Internet host:

CLI

```
# exec ping www.yahoo.com
PING ds-fp3.wg1.b.yahoo.com (206.190.36.45): 56 data bytes
64 bytes from 206.190.36.45: icmp_seq=0 ttl=52 time=220.2 ms
64 bytes from 206.190.36.45: icmp_seq=1 ttl=52 time=230.0 ms
64 bytes from 206.190.36.45: icmp_seq=2 ttl=52 time=222.2 ms
64 bytes from 206.190.36.45: icmp_seq=3 ttl=52 time=238.3 ms
64 bytes from 206.190.36.45: icmp_seq=4 ttl=52 time=263.2 ms

--- ds-fp3.wg1.b.yahoo.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 220.2/234.7/263.2 ms
```

UPDATE YOUR SECURITY SERVICES DATABASES

Once your unit has access to Internet is the right time to update your FortiGate's security services databases. Having up-to-date databases and engines is a key part of the Proof of Concept as this will improve catch-rates, performance and customer overall impression.

As first step you should configure Antivirus to use the "normal" database

CLI

```
config antivirus settings
    set default-db normal
end
```

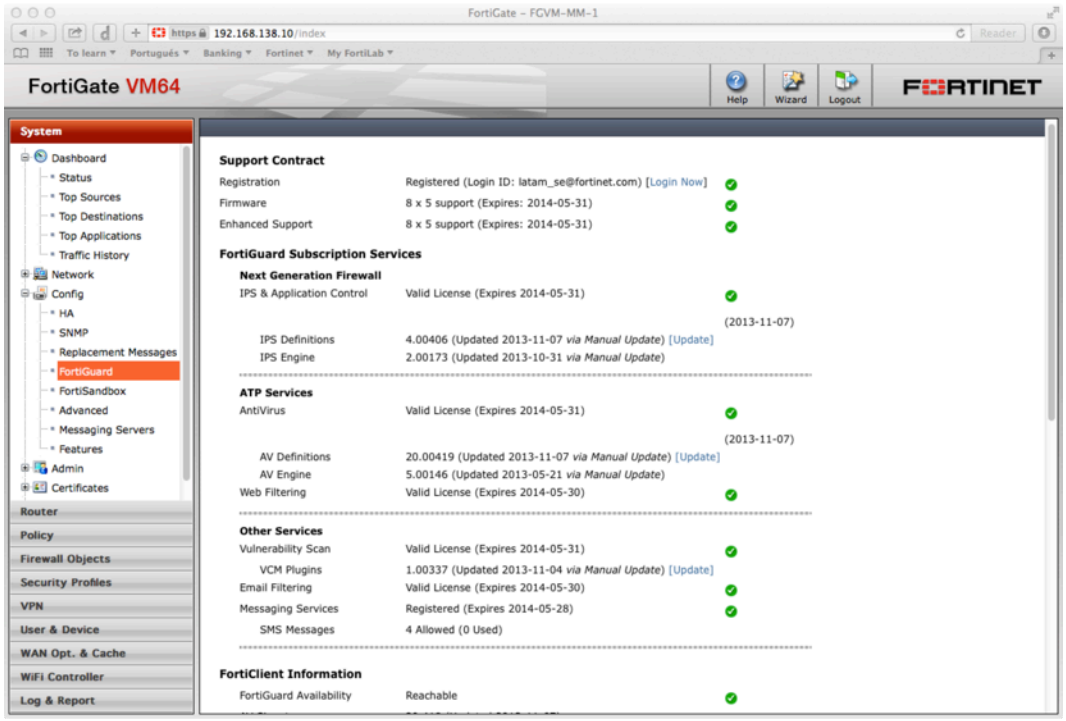
Update FortiGuard signatures and engines.

CLI

```
# exec update-now
```

GUI

1. Go to System → Config → FortiGuard
2. Expand the “AV & IPS Download Options” section and click on “Update Now”
3. Make sure FortiGuard Subscription Services appear with a green check mark.



NOTE

By default, FortiGate uses port UDP/53 for communicating with the FortiGuard servers. It might be the case that a filtering device blocks this traffic for not being DNS (e.g. a DPI in the network). If that's the case, you have the option of using port UDP/8888

CONFIGURE TRAFFIC INTERFACE (SNIFFER)

Configure the interface that is going to be wired to the SPAN/Mirror port in the switch.

Remember to delete any reference (policies, routes, etc.) to the interface before changing it to sniffer-mode.

BEST PRACTICE TIP

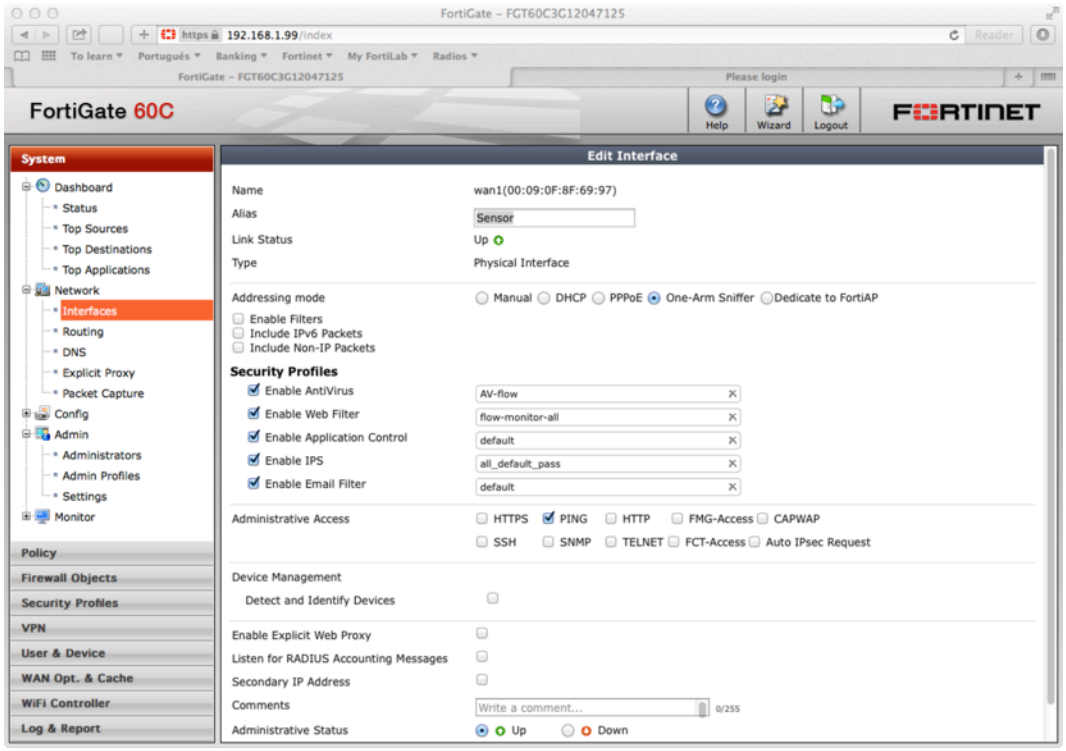
Using different interfaces for sniffing and management is recommended

CLI

```
config system interface
    edit "wan1"
        set vdom "root"
        set allowaccess ping
        set ips-sniffer-mode enable
        set type physical
        set alias "Sensor"
        set snmp-index 2
    next
end
```

GUI

1. Go to System → Network → Interfaces
2. Select appropriate traffic interface.
3. Select “One-Arm Sniffer” as Addressing Mode
4. OK



CONFIGURE SECURITY PROFILES

In the next steps we will configure security profiles that will be used for traffic inspection. Be aware in that when running in sniffer mode only “flow-based” security profiles should be used, as there’s no possibility of proxies to intercept connection on this mode.

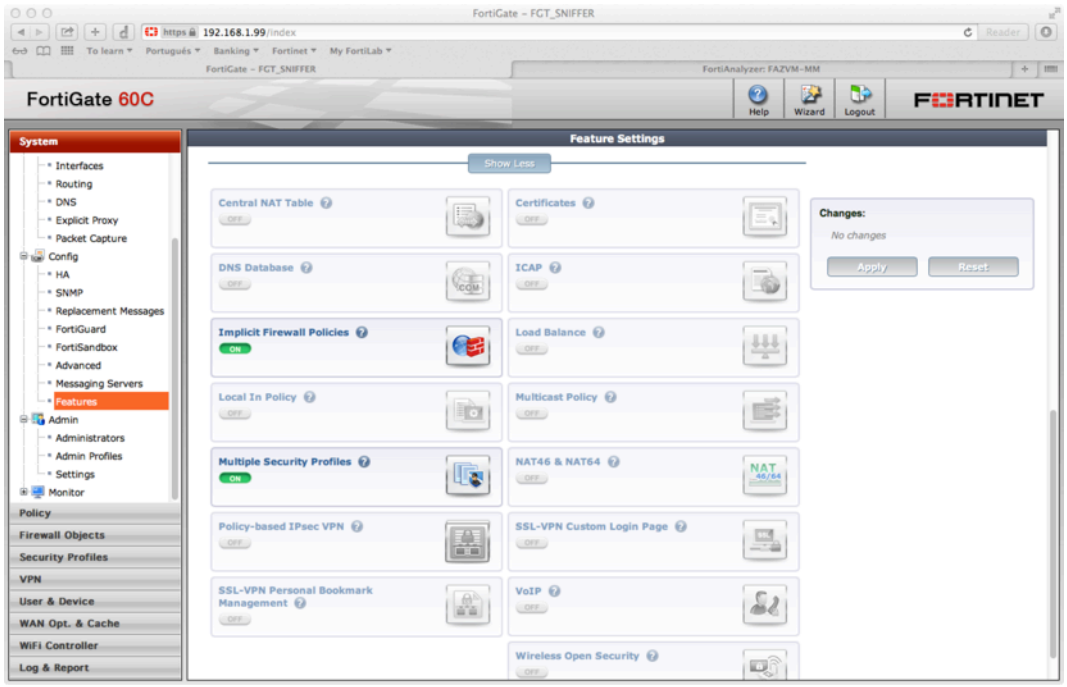
Enable multiple UTM profiles: If you’re using an entry level FortiGate you will probably have to enable the use of multiple UTM profiles, as by default just one profile per functionality can be configured.

CLI

```
config system global
    set gui-multiple-utm-profiles enable
end
```

GUI

1. Go to System → Config → Features
2. Click on “Show More”
3. Enable Multiple Security Profiles
4. Apply



For the purpose of this document we will use FortiGate pre-configured profiles and highlight in bold letter any alteration you need to do from the default.

Antivirus Profile:

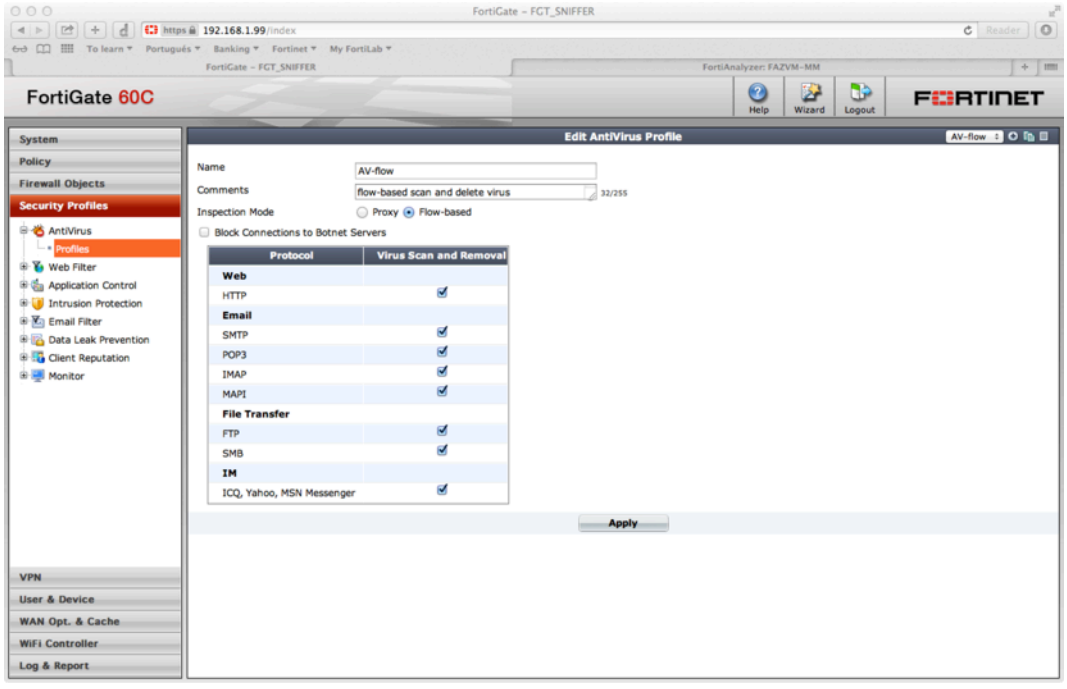
CLI

```
config antivirus profile
    edit "AV-flow"
        set comment "flow-based scan and delete virus"
        set inspection-mode flow-based
        set extended-utm-log enable
            config http
                set options scan
            end
            config ftp
                set options scan
            end
            config imap
                set options scan
            end
            config pop3
                set options scan
            end
            config smtp
                set options scan
            end
            config mapi
                set options scan
            end
            config nntp
                set options scan
            end
            config im
                set options scan
            end
            config smb
```

```
                set options scan
            end
        set av-virus-log enable
        set av-block-log enable
    next
end
```

GUI

1. Go to Security Profiles → Antivirus → Profiles
2. Select AV-flow
3. Enable IMAP and SMB support
4. Apply



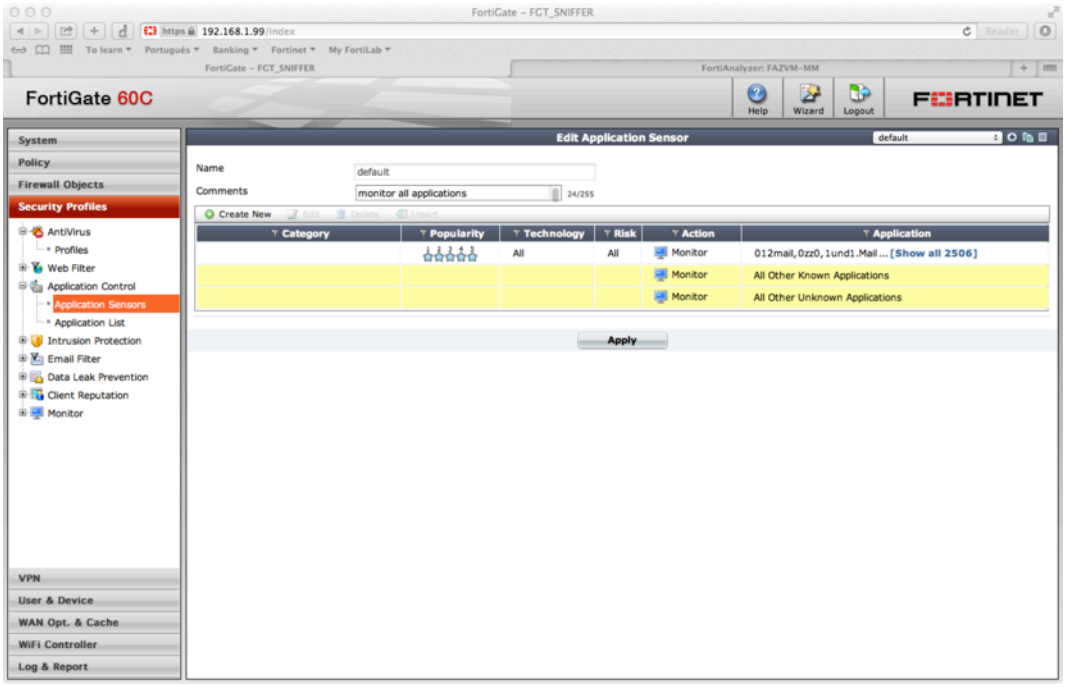
Configure Application Control sensor:

CLI

```
config application list
    edit "default"
        set comment "monitor all applications"
        set extended-utm-log enable
        set other-application-log enable
        set log enable
        set unknown-application-log enable
            config entries
                edit 1
                    set action pass
                next
            end
    next
end
```

GUI

1. Go to Security Profiles → Application Control → Application Sensors
2. Select “default”
3. Apply



Configure Web Filtering profile:

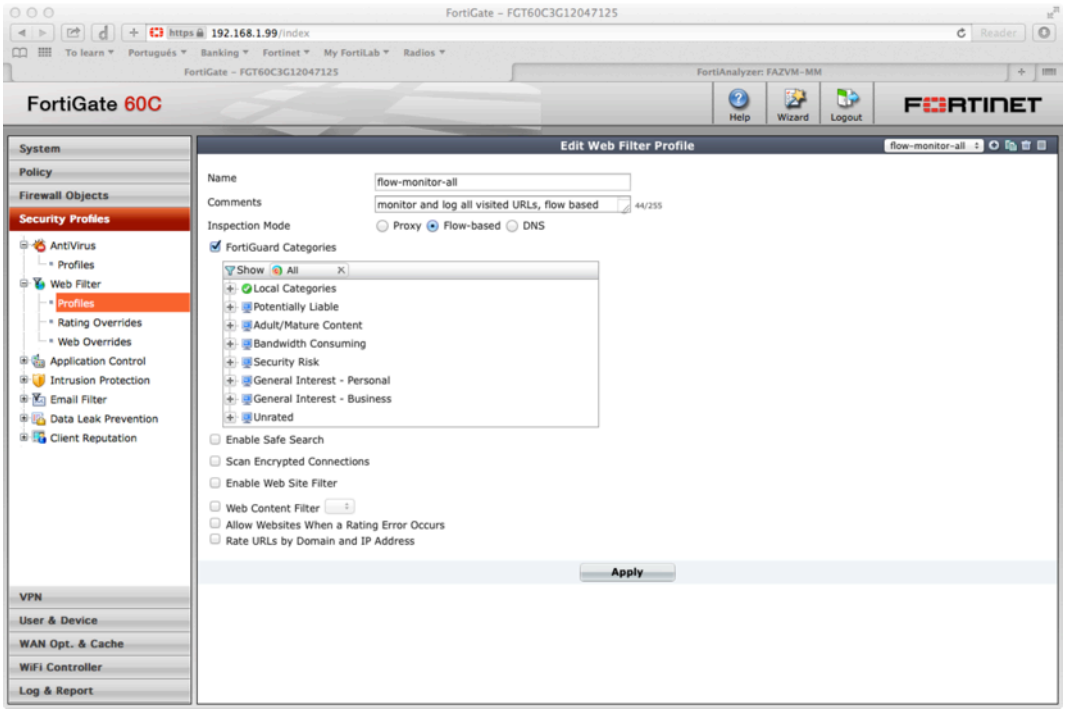
CLI

```
config webfilter profile
    edit "flow-monitor-all"
        set comment "monitor and log all visited URLs, flow
based"
        set extended-utm-log enable
        set inspection-mode flow-based
        set options https-url-scan
            config ftgd-wf
                unset options
                unset exempt-ssl
                    config filters
                        edit 1
                            set category 1
```

```
                        next
                          (…
                          other categories the same
                          …)
                        edit 78
                            set category 84
                        next
                        edit 79
                        next
                    end
            end
        set log-all-url enable
        set web-content-log disable
        set web-filter-activex-log disable
        set web-filter-command-block-log disable
        set web-filter-cookie-log disable
        set web-filter-applet-log disable
        set web-filter-jscript-log disable
        set web-filter-js-log disable
        set web-filter-vbs-log disable
        set web-filter-unknown-log disable
        set web-filter-referer-log disable
        set web-filter-cookie-removal-log disable
        set web-url-log disable
        set web-invalid-domain-log disable
        set web-ftgd-err-log disable
        set web-ftgd-quota-usage disable
    next
end
```

GUI

1. Go to Security Profiles → Web Filter → Profiles
2. Select “flow-monitor-all”
3. Apply



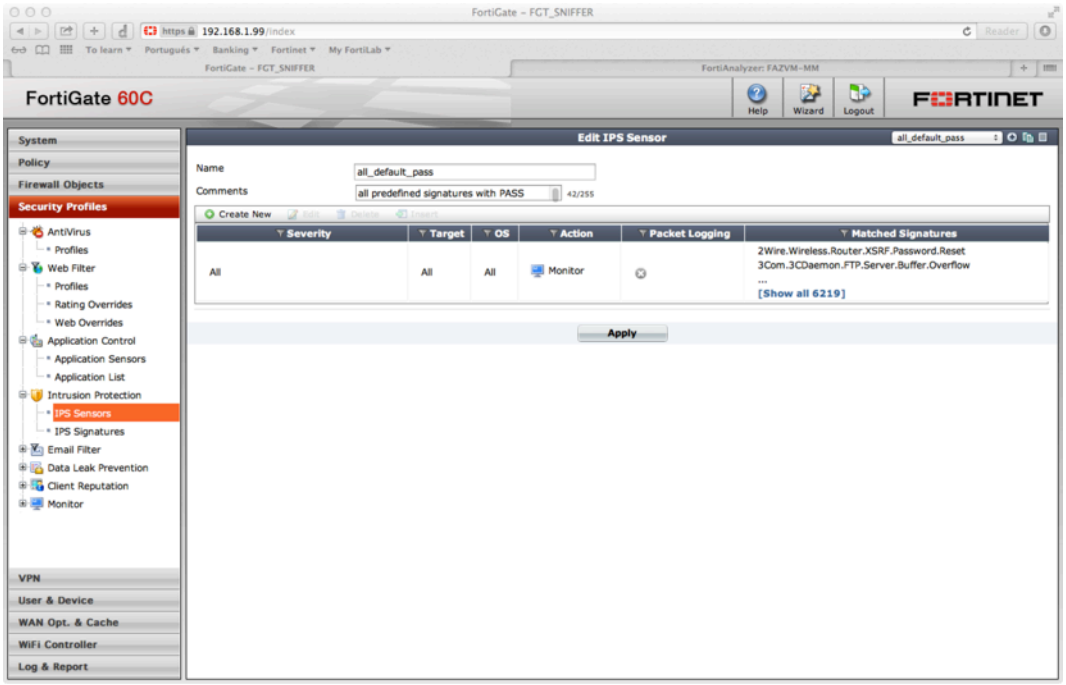
Configure IPS Sensor:

CLI

```
config ips sensor
    edit "all_default_pass"
        set comment "all predefined signatures with PASS
action"
            config entries
                edit 1
                    set action pass
                next
            end
    next
end
```

GUI

1. Go to Security Profiles → Intrusion Prevention → IPS Sensor
2. Select “all_default_pass”
3. Apply

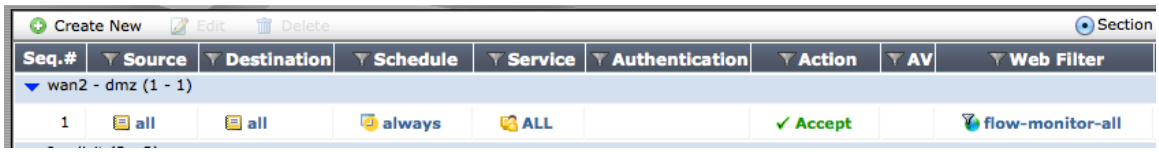


CONFIGURE SNIFFER POLICY

Once the basic networking has been configured and has been defined security profiles, we just need to put both things together. Creating a special kind of policies known as “sniffer policies” does this.

IMPORTANT TIP

In case you want to generate reports containing URL Filtering categories make sure you create a policy containing a Web Filtering profile. FortiGuard rating won't be enabled unless a policy containing a Web Filtering profile is defined.



This tricky configuration has been identified and acknowledged for a future enhancement.

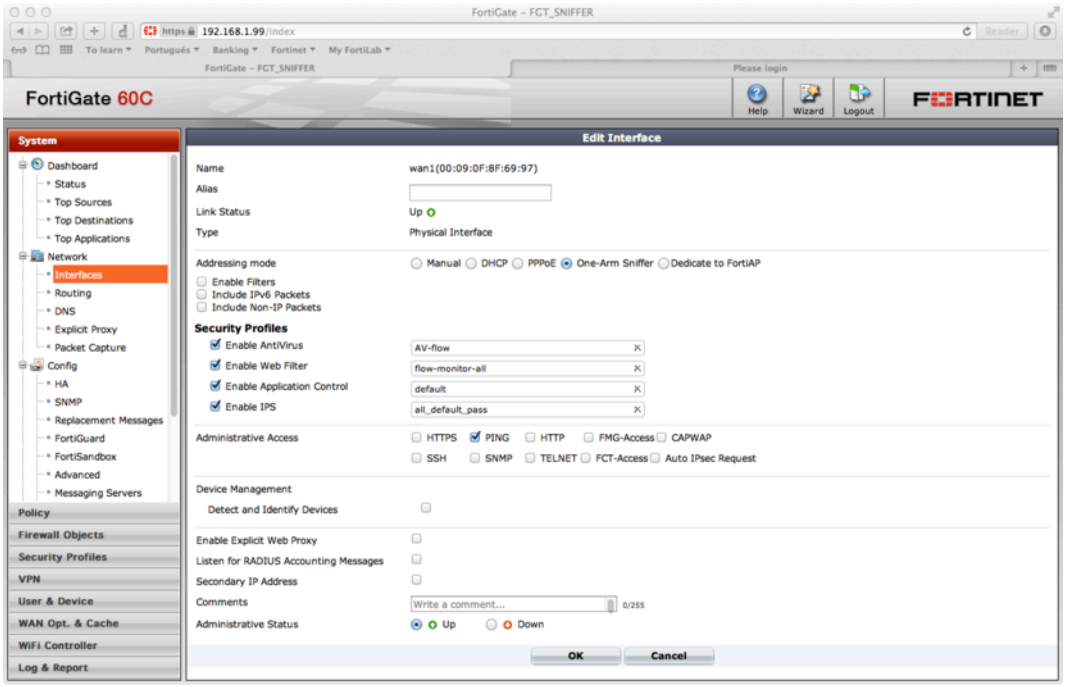
CLI

```
config firewall sniffer
    edit 0
        set logtraffic all
        set interface "wan1"
        set application-list-status enable
        set application-list "default"
        set ips-sensor-status enable
        set ips-sensor "all_default_pass"
        set av-profile-status enable
        set av-profile "AV-flow"
        set webfilter-profile-status enable
        set webfilter-profile "flow-monitor-all"
    next
end
```

GUI

1. Go to System → Network → Interfaces
2. Edit appropriate traffic interface.

3. Enable Security Profiles for Antivirus, Web Filter, Application Control and IPS, select recently configured profiles
4. OK



HANDS-ON: FORTIANALYZER CONFIGURATION

In order to provide better visibility and full reporting we will integrate the FortiGate device with a FortiAnalyzer. Let's remember FortiAnalyzer is the security architecture component that allows for a more professional reporting, compared to the basic reporting done by the FortiGate.

CONFIGURE FORTIGATE LOGGING TO FORTIANALYZER

CLI

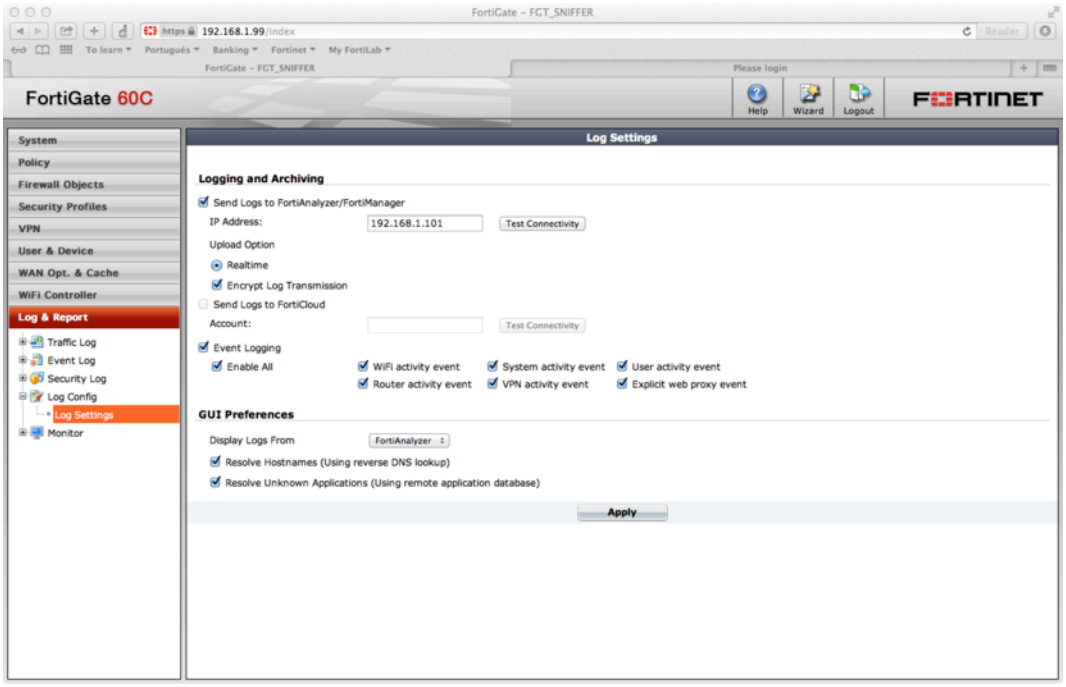
```
config log fortianalyzer setting
    set status enable
    set server 192.168.1.101
    set reliable enable
end
```

GUI

1. Go to Log & Report → Log Config → Log Settings
2. Enable "Send Logs to FortiAnalyzer/FortiManager"
3. Configure FortiAnalyzer's IP address
4. Apply

NOTE

When doing "Test Connectivity" you might get an error as the Device hasn't been accepted in the FortiAnalyzer yet.

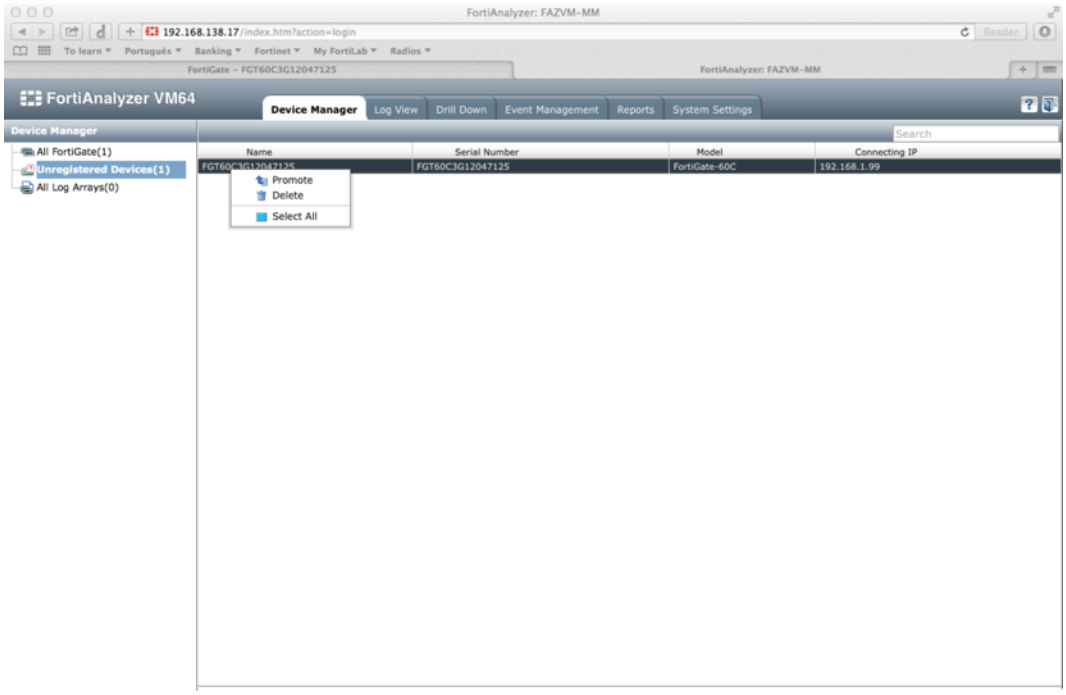


CONFIGURE FORTIANALIZER FOR ACCEPTING FORTIGATE LOGGING

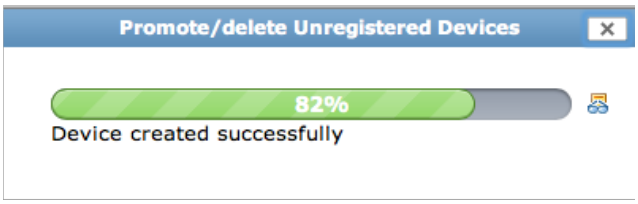
After configuring the FortiGate to send logs to FortiAnalyzer, you will need to accept the devices as logging resource. This is done from FortiAnalyzer's GUI.

GUI

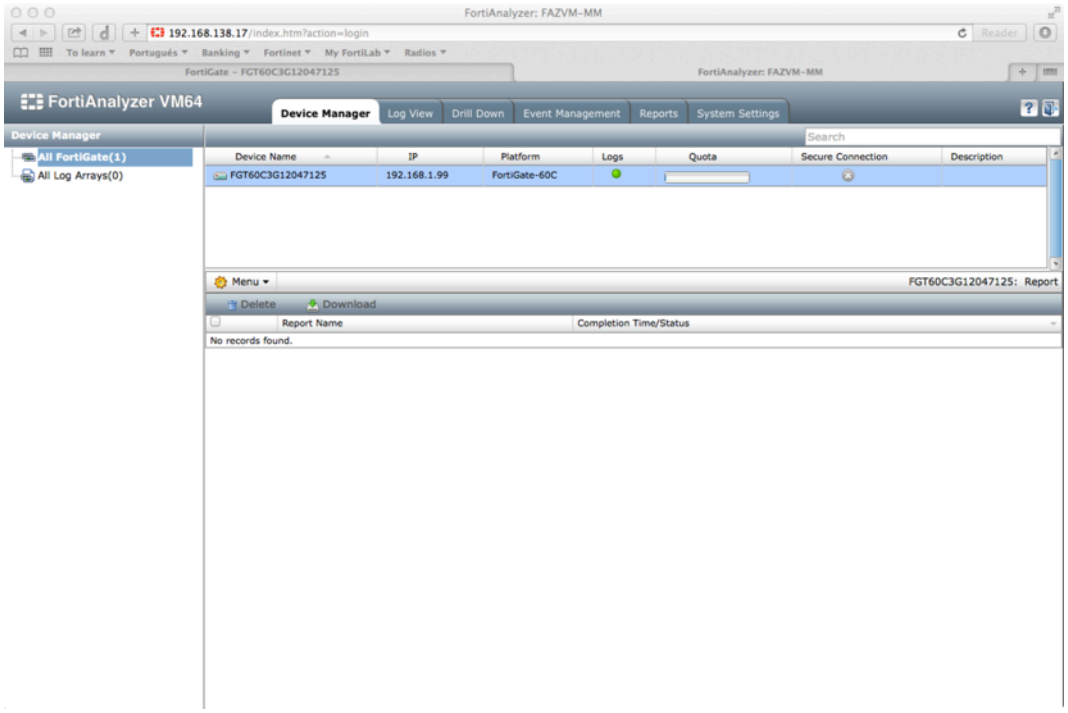
1. Login to FortiAnalyzer GUI using HTTP/S
2. Go to Device Manager tab
3. Look into "Unregistered Devices" list
4. Make sure you select the proper FortiGate in the list, right-click and select "Promote" from the list.



5. Wait until the process finish.



6. Verify your FortiGate appears listed as an accepted device.


FortiAnalyzer: FAZVM-MM
192.168.138.17/index.htm?action=login
FortiAnalyzer VM64
Device Manager
Log View
Drill Down
Event Management
Reports
System Settings
Device Manager
All FortiGate(1)
All Log Arrays(0)
Search
Device Name
IP
Platform
Logs
Quota
Secure Connection
Description
FGT60C3G12047125
192.168.1.99
FortiGate-60C
Menu
FGT60C3G12047125: Report
Delete
Download
Report Name
Completion Time/Status
No records found.

HANDS-ON: PUTTING ALL TOGETHER – NETWORK CONFIGURATION

Once FortiGate and FortiAnalyzer have configured the last step would be setting up the network in order to send traffic to the FortiGate.

CONFIGURE SWITCH

The FortiGate will receive traffic from a networking switch. First thing to understand is that because of this the FortiGate will only have visibility of traffic being redirected by this switch.

For the purpose of this Proof of Concept (POC) the recommendation would be to plug the FortiGate to the switch that receives all Internet facing traffic.

Configure SPAN/Mirror port:

This activity has to be done by company's networking specialists.

In order for FortiGate to get appropriate information, provides visibility and reporting, traffic in both directions should be copied/mirrored.

VERIFY CONFIGURATION

Using network sniffer:

Once the switch has been configured everything is ready to start inspecting traffic. Before getting into graphics and reporting make sure you verify that FortiGate is actually receiving traffic. This can be done by running a TCP dump on sniffing configured interface:

CLI

```
# diagnose sniffer packet wan1 '' 1
interfaces=[wan1]
filters=[]
0.592415 200.42.92.139.1935 -> 192.168.1.44.53307: psh
2596606569 ack 2829680690
0.592770 192.168.1.44.53307 -> 200.42.92.139.1935: ack
2596606587
…
…
…

66 packets received by filter
0 packets dropped by kernel
```

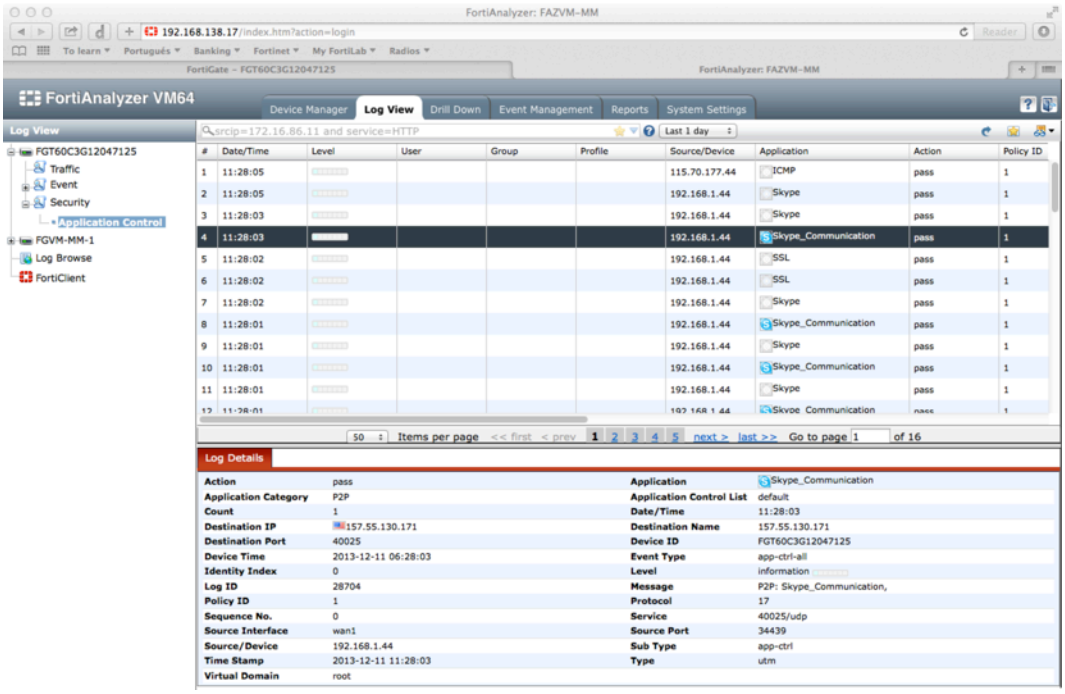
HANS-ON: REVIEWING LOGS AND GENERATING REPORTS

Once your FortiGate and your networking device are configured you will be able to view logs, filter them and create reports. We will not go through the process of generating new reports but using a predefined one that has to be imported into the FortiAnalyzer.

VIEWING LOS IN FORTIANALYZER

GUI

1. Login to FortiAnalyzer using HTTPS
2. Go to Log View tab
3. On left pane, select your FortiGate's name → Security → Application Control (other logs can be used for this example)
4. On right pane you should see a list of the log entries
5. Select any entry a see details below.



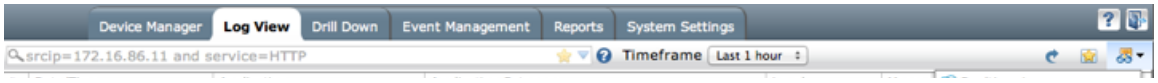
Filtering logs in FortiAnalyzer

GUI

There're two ways of using filters with FortiAnalyzer 5.0.3:

1. Using the top filtering bar

   Top filtering bar allows you to use free text in combination with some tags in order to search for records in an easy and fast way



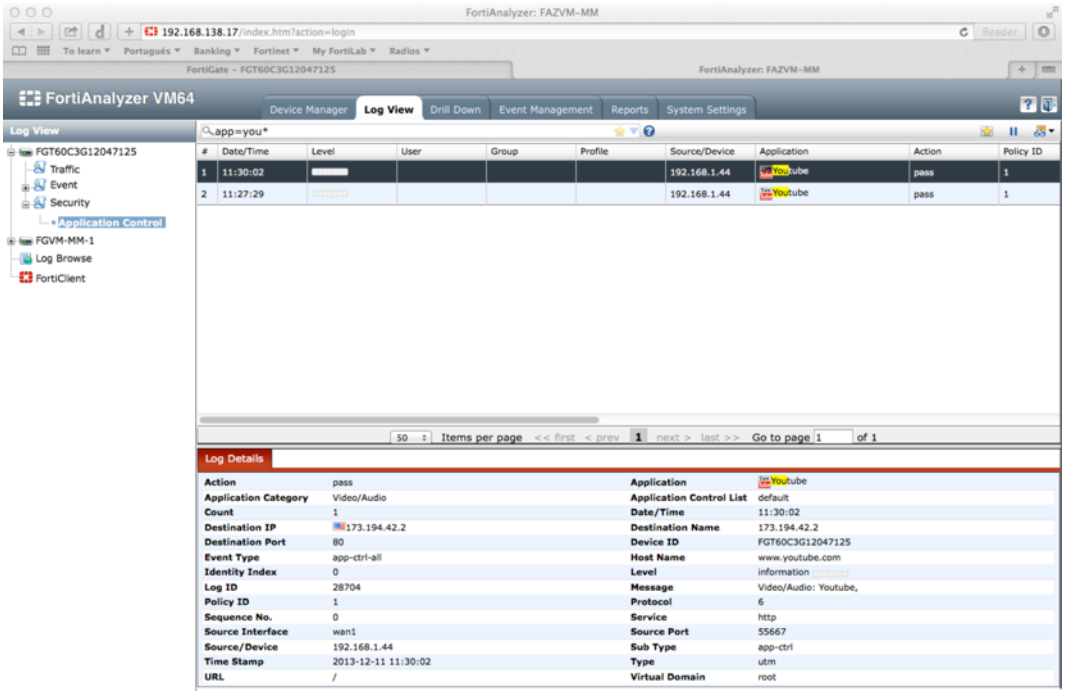
   Some example of searches you could do:

   - app=dns

- app=youtu*
- apptype=vide*
- dstport=80 and srcip=192.168.1.*

NOTE

In order to ease your free text search, make sure you set “Case Insensitive Search” using View Options ( ) button.

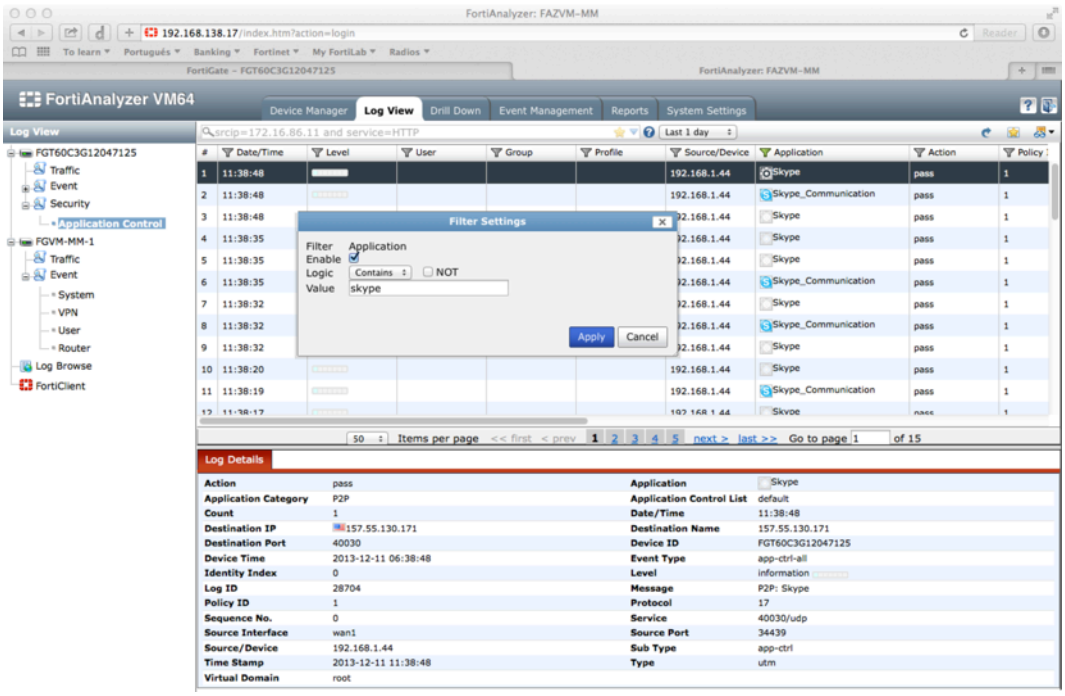


2. Using column filters

   Column filters the traditional way of filtering records by specifying the desired value on each column. When filter in more than one column are specified they are joined by a logical AND, so all filter has to be true in

NOTE

Column filters are not enabled by default. Click on View Options ( ) button and enable them.



Click on the filter icon over the column to specify the desire value for it.

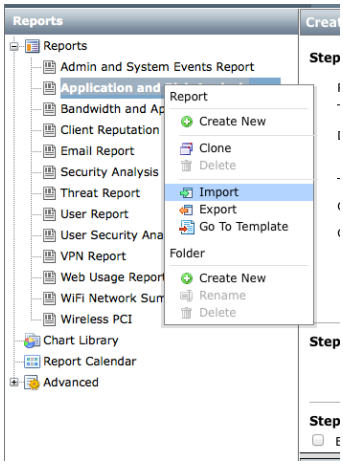
GENERATING REPORTS IN FORTIANALYZER

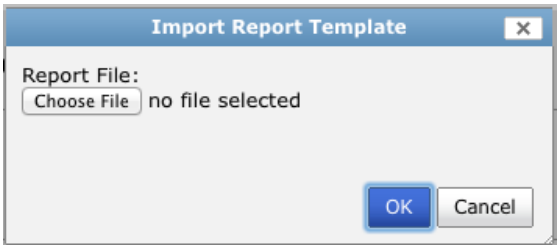
This section will show how to use and generate pre-configured reports. Generating new reports is outside the scope of this document.

For the sake of this POC we will use a special report created specifically for devices capturing traffic in one-arm mode, “Application and Risk Analysis – One Arm”.

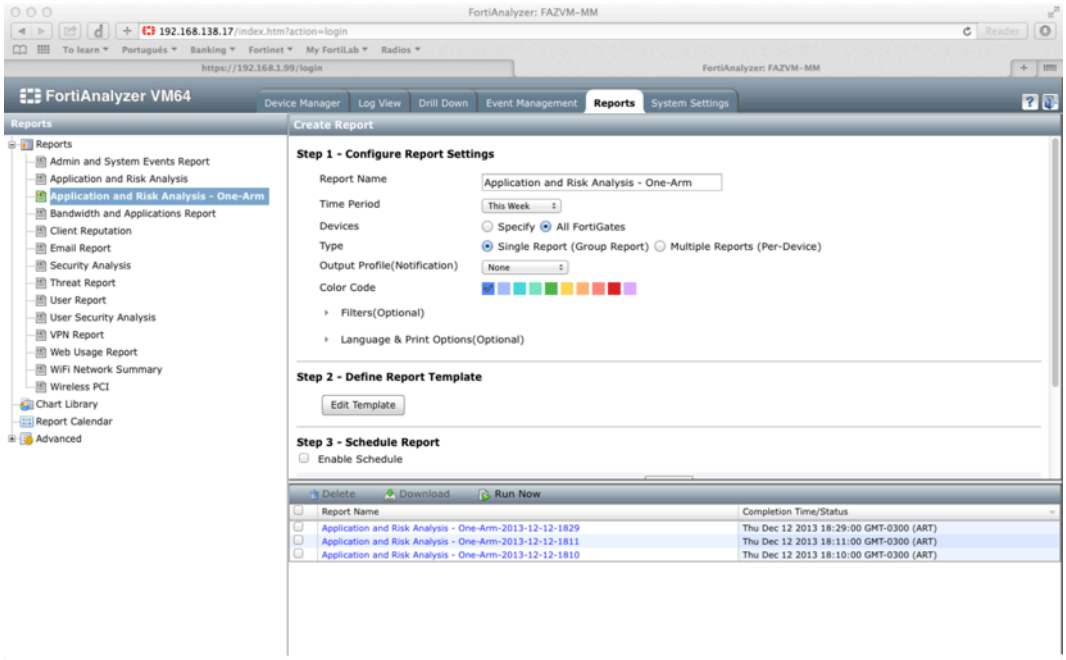
GUI

1. Go to Reports tab
2. Right click in any of the predefined reports and select “Import”

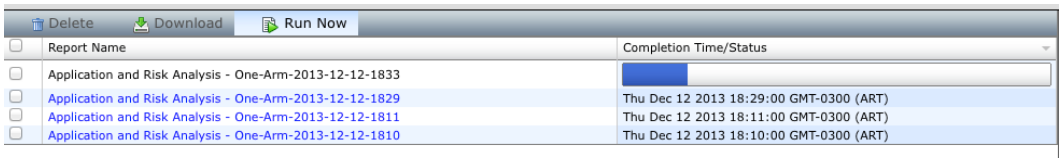




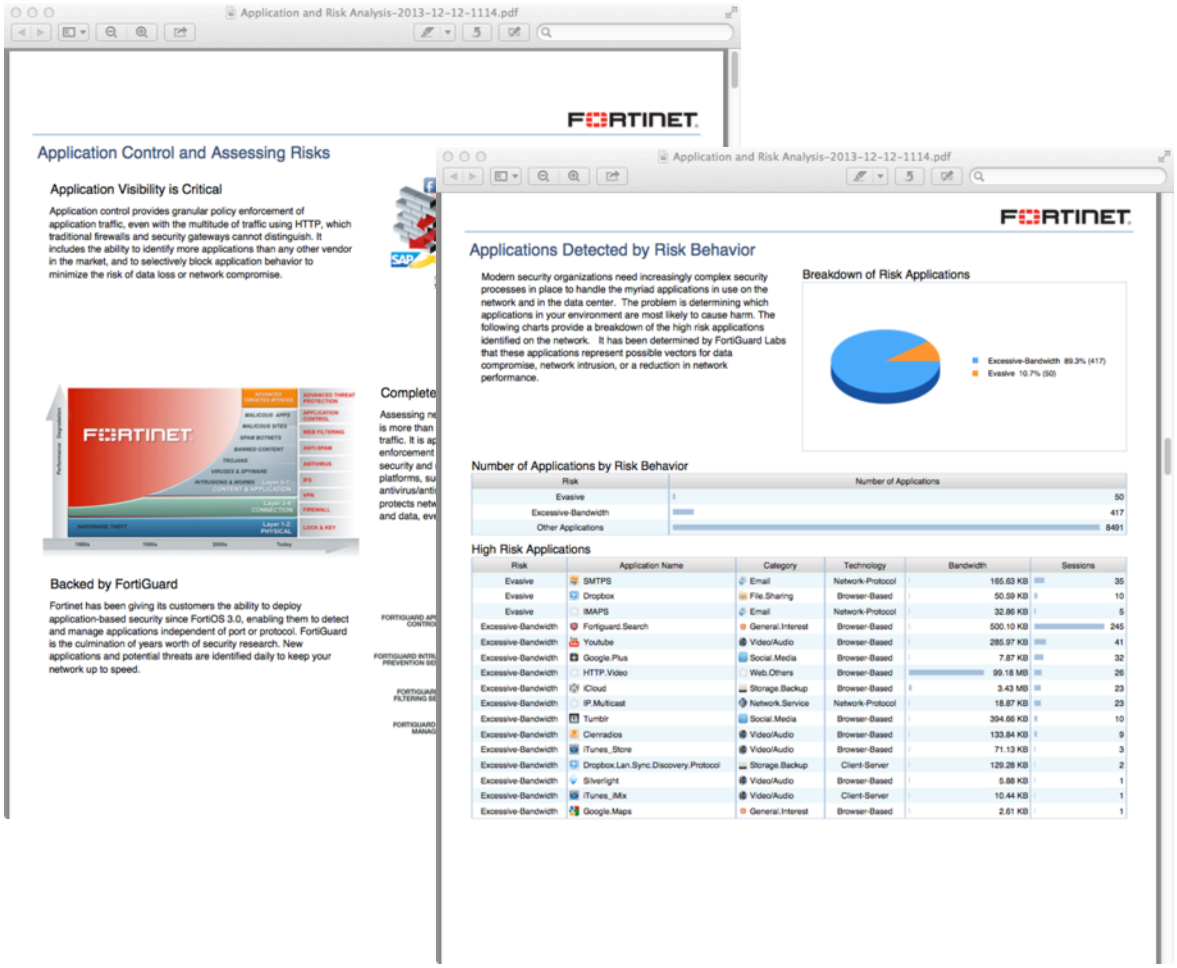
3. Search and select “Application and Risk Analysis – One Arm.dat” in the choose file dialog. Then click OK.
4. Once the report has been imported. Go to Reports → Application and Risk Analysis – One Arm
5. Select the “Time Period” of your choice according to the time the device has been collecting logs.
6. Devices: All FortiGates



7. Click Apply and then Run Now



8. Wait until the reports has been generated and click on the report link to visualize it or choose the download button to get a PDF version of it
9. Provide the customer with generated report.


Application and Risk Analysis-2013-12-12-1114.pdf
Application Control and Assessing Risks
Application Visibility is Critical
Application control provides granular policy enforcement of application traffic, even with the multitude of traffic using HTTP, which traditional firewalls and security gateways cannot distinguish. It includes the ability to identify more applications than any other vendor in the market, and to selectively block application behavior to minimize the risk of data loss or network compromise.
Backed by FortiGuard
Fortinet has been giving its customers the ability to deploy application-based security since FortiOS 3.0, enabling them to detect and manage applications independent of port or protocol. FortiGuard is the culmination of years worth of security research. New applications and potential threats are identified daily to keep your network up to speed.
Application and Risk Analysis-2013-12-12-1114.pdf
Applications Detected by Risk Behavior
Modern security organizations need increasingly complex security processes in place to handle the myriad applications in use on the network and in the data center. The problem is determining which applications in your environment are most likely to cause harm. The following charts provide a breakdown of the high risk applications identified on the network. It has been determined by FortiGuard Labs that these applications represent possible vectors for data compromise, network intrusion, or a reduction in network performance.
Breakdown of Risk Applications
Excessive-Bandwidth 89.3% (417)
Evasive 10.7% (50)
Number of Applications by Risk Behavior
Risk
Number of Applications
Evasive 50
Excessive-Bandwidth 417
Other Applications 8491
High Risk Applications
Risk
Application Name
Category
Technology
Bandwidth
Sessions
Evasive SMTPS Email Network-Protocol 165.63 KB 35
Evasive Dropbox File.Sharing Browser-Based 50.59 KB 10
Evasive IMAPS Email Network-Protocol 32.86 KB 5
Excessive-Bandwidth Fortiguard.Search General.Interest Browser-Based 500.10 KB 245
Excessive-Bandwidth Youtube Video/Audio Browser-Based 285.97 KB 41
Excessive-Bandwidth Google.Plus Social.Media Browser-Based 7.87 KB 32
Excessive-Bandwidth HTTP.Video Web.Others Browser-Based 99.18 MB 26
Excessive-Bandwidth iCloud Storage.Backup Browser-Based 3.43 MB 23
Excessive-Bandwidth IP.Multicast Network.Service Network-Protocol 18.87 KB 23
Excessive-Bandwidth Tumblr Social.Media Browser-Based 394.66 KB 10
Excessive-Bandwidth Cienradios Video/Audio Browser-Based 133.84 KB 9
Excessive-Bandwidth iTunes_Store Video/Audio Browser-Based 71.13 KB 3
Excessive-Bandwidth Dropbox.Lan.Sync.Discovery.Protocol Storage.Backup Client-Server 129.28 KB 2
Excessive-Bandwidth Silverlight Video/Audio Browser-Based 5.88 KB 1
Excessive-Bandwidth iTunes_iMix Video/Audio Client-Server 10.44 KB 1
Excessive-Bandwidth Google.Maps General.Interest Browser-Based 2.61 KB 1

APPENDIX I – SNIFFER MODE – POC CHECK LIST

STEP ZERO

- ☐ Do all this procedure on a controlled network (your own company network!) at least once before attempting this on a customer's network.

BEFORE DOING ANY CONFIGURATION

- ☐ Call the customer. Gather every information you will need during the POC
- ☐ Make sure products are registered, with valid FortiGuard contracts and proper FortiOS versions.
- ☐ Make sure paperwork has been done and that you won't have any logistic issue to get the equipment inserted into the customer's network

CONFIGURING THE FORTIGATE

- ☐ Do a factory reset
- ☐ Configure networking: Management interface, DNS, default gateway and other routes. Test your networking configuration
- ☐ Update FortiGuard signatures and engines
- ☐ Configure sniffing interface
- ☐ Configure security profiles: Antivirus, Application Control, Web Filtering, IPS
- ☐ Configure sniffing policy

CONFIGURING THE FORTIANALYZER

- ☐ Setup FortiAnalyzer
- ☐ Configure FortiGate to send logs to FortiAnalyzer
- ☐ Setup networking (switch, router) so traffic gets copied to FortiGate.
- ☐ Verify that the FortiGate is receiving network traffic
- ☐ Review logs and generate reports
- ☐ Provide customer with generated reports
- ☐ Make sure you provide a follow-up email/report summarizing the results of the POC.
- ☐ Sell!

APPENDIX II – REFERENCES

- CLI Reference Guide for FortiOS 5.0
  http://docs.fortinet.com/fgt/handbook/50/5-0-4/fortigate-cli-50.pdf

- Install and System Administration for FortiOS 5.0
  http://docs.fortinet.com/fgt/handbook/50/5-0-4/fortigate-install-system-admin-50.pdf

- Security Profiles for FortiOS 5.0
  http://docs.fortinet.com/fgt/handbook/50/fortigate-security_profiles-50.pdf

- The FortiOS Handbook
  http://docs.fortinet.com/fgt/handbook/50/fortios-handbook-50.pdf

- FortiAnalyzer v5.0 Administration Guide
  http://docs.fortinet.com/fa/50/FortiAnalyzer-504-Admin-Guide.pdf

- The FortiGate Cookbook
  http://docs.fortinet.com/cookbook.html

- Administration Guide
  http://docs.fortinet.com/fa/50/FortiAnalyzer-504-Admin-Guide.pdf